011416809 **Image available**
WPI Acc No: 1997-394716/199737
XRPX Acc No: N97-328450
Transmission data integrity and authentication method - using same algorithm as source to derive integrity mark, and compares both integrity marks and in case of agreement sends notice to source with decoded code integrity mark
Patent Assignee: DEUT TELEKOM AG (DEBP)
Inventor: ENDRES H; GEYER K
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
DE 19604150	A1	19970807	DE 1004150	A	19960206	199737 B

Priority Applications (No Type Date): DE 1004150 A 19960206
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 19604150	A1		6		

Abstract (Basic): DE 19604150 A

The method selects the document to be transmitted, from memory, and prepares (3) a signature of the document (SIGN). the signature is then encoded (4) to form (5) the integrity mark (VAR) from the coded document (DSC). A part (IK) of the coded document is then separated (6).

A transaction variable (TAV) is formed and additional information (ADINFO) is added (8). The additional information contains the date and the time of day. All the information is made into a data bank, and provided with an envelope and signature (ES). The document (DSC) and envelope (ESC) are then transmitted.

USE/ADVANTAGE - E.g. for data communication system. Improves security and reliability of data transmission.

Dwg.1/2

Title Terms: TRANSMISSION; DATA; INTEGRITY; AUTHENTICITY; METHOD; ALGORITHM ; SOURCE; DERIVATIVE; INTEGRITY; MARK; COMPARE; INTEGRITY; MARK; CASE; AGREE; SEND; NOTICE; SOURCE; DECODE; CODE; INTEGRITY; MARK
Derwent Class: W01
International Patent Class (Main): H04L-009/32
International Patent Class (Additional): H04L-001/12
File Segment: EPI
Manual Codes (EPI/S-X): W01-A01A; W01-A05B

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 04 150 A 1**

(51) Int. Cl.[6]:
H 04 L 9/32
H 04 L 1/12

(21) Aktenzeichen: 196 04 150.3
(22) Anmeldetag: 6. 2. 96
(43) Offenlegungstag: 7. 8. 97

DE 196 04 150 A 1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

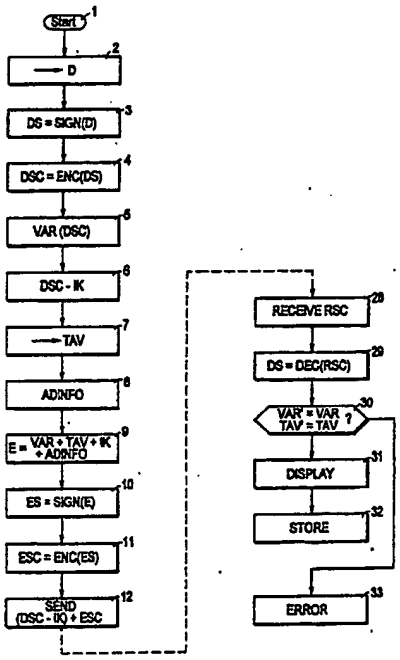
(72) Erfinder:
Endres, Helmut, Dipl.-Ing., 96148 Baunach, DE;
Geyer, Klaus, Dipl.-Ing., 97456 Dittelbrunn, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 44 13 678 C1
Prospekt: Telesec, Kommunikationssicherheit, Telekom, Siegen, 1994, S.8,9;

(54) Verfahren zur Bestätigung des Empfangs einer übertragenen Nachricht

(57) Bei einem Verfahren zur integren und authentischen Bestätigung des Empfangs einer von einem Absender an einen Empfänger übertragenen Nachricht ist vorgesehen, daß absenderseitig aus der Nachricht ein Integritätsmerkmal abgeleitet wird, das als Integritätsmeldung für den Empfänger entschlüsselbar verschlüsselt zum Empfänger übertragen wird, daß empfängerseitig das verschlüsselte Integritätsmerkmal entschlüsselt wird, daß aus der empfangenen Nachricht mit dem sendeseitig angewandten Algorithmus das Integritätsmerkmal abgeleitet wird, daß das entschlüsselte und das empfängerseitig abgeleitete Integritätsmerkmal miteinander verglichen werden und daß bei Übereinstimmung eine Rückmeldung an den Absender übertragen wird, die in für den Absender entschlüsselbarer verschlüsselter Form das Integritätsmerkmal enthält.



DE 196 04 150 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur integren und authentischen Bestätigung des Empfangs einer von einem Absender an einen Empfänger übertragenen Nachricht.

Der Versand von Dokumenten auf elektronischem Wege wird derzeit so durchgeführt, daß vom Absender ein Kennzeichen mitgeschickt wird, welches den Empfänger darauf hinweist, eine Empfangsbestätigung abzusenden. Ferner wird vom Absender eine Zufallszahl mitgeschickt, die beim Zurücksenden den Nachweis erbringen soll, daß das Dokument angekommen ist. Hiermit ist jedoch weder beweisbar, daß das Dokument beim vorgesehenen Empfänger und nicht bei einem anderen Empfänger angekommen ist, noch daß das Dokument unverfälscht beim Empfänger eingetroffen ist.

Aufgabe der vorliegenden Erfindung ist es, den ordnungsgemäßen Empfang durch den richtigen Empfänger dem Absender zu bestätigen. Die erfindungsgemäße Aufgabe wird dadurch gelöst,

- daß absenderseitig aus der Nachricht ein Integritätsmerkmal abgeleitet wird, das als Integritätsmeldung für den Empfänger entschlüsselbar verschlüsselt zum Empfänger übertragen wird,
- daß empfängerseitig das verschlüsselte Integritätsmerkmal entschlüsselt wird,
- daß aus der empfangenen Nachricht mit dem sendeseitig angewandten Algorithmus das Integritätsmerkmal abgeleitet wird,
- daß das entschlüsselte und das empfängerseitig abgeleitete Integritätsmerkmal miteinander verglichen werden und
- daß bei Übereinstimmung eine Rückmeldung an den Absender übertragen wird, die in für den Absender entschlüsselbarer verschlüsselter Form das Integritätsmerkmal enthält.

Das erfindungsgemäße Verfahren hat den Vorteil, daß integer bestätigt wird, daß der für den Empfang vorgesehene Empfänger das Dokument mit dem abgesandten Inhalt erhalten hat. Zur Ableitung des Integritätsmerkmals sind verschiedene Verfahren bekannt, beispielsweise Prüfsummen und die Bildung von Hash-Werten oder Session-Keys. Gegenüber dem postalischen Verfahren "Einschreiben mit Rückschein" hat das erfindungsgemäße Verfahren den Vorteil, daß nicht der Empfang mit irgendeinem Inhalt, sondern zutreffendenfalls der Empfang des abgesandten Dokuments bestätigt wird.

Die im Rahmen des erfindungsgemäßen Verfahrens übertragenen Nachrichten sind in erster Linie solche, die zwar als gespeicherte, computer-lesbare Dateien vorliegen, jedoch auch in ausgedruckter Form herkömmliche Dokumente bilden, wie beispielsweise Urkunden, Geschäftsbriefe, technische Zeichnungen und Bilder. Das erfindungsgemäße Verfahren ist jedoch auch auf solche Nachrichten anwendbar, die nicht oder kaum menschenlesbar sind oder nicht in dauerhafter Papierform vorliegen, wie beispielsweise Computerprogramme in Maschinencode oder Schallereignisse.

Mit dem erfindungsgemäßen Verfahren können überall dort Dokumente mit einer Empfangsbestätigung übersandt werden, wo es auf eine Dokumentation des Erhalts ankommt, also beispielsweise bei Anwälten, Gerichten, Notaren, Behörden, Unternehmen, Politikern und Steuerberatern. Die absenderseitig und empfängerseitig notwendigen Verfahrensschritte können durch geeignete Computer-Programme bedienergeführt vollzogen werden. Die dabei erforderliche Eingabe der geheimen Daten, wie beispielsweise geheime Schlüssel oder Signaturen, können in Chipkarten abgespeichert sein und bei Bedarf mit Hilfe von Lesegeräten gelesen und verwendet werden.

Zur Verschlüsselung der Integritätsmeldung und der Rückmeldung stehen ebenfalls verschiedene bekannte Verfahren zur Verfügung. So kann beispielsweise zusätzlich zu einem symmetrischen Schlüssel ein asymmetrischer Schlüssel verwendet werden, bei dem jedem beteiligten Absender und Empfänger ein allgemein bekannter, öffentlicher Schlüssel (Public Key) und ein geheimer Schlüssel (Secret Key) zugeteilt ist. Der Absender verschlüsselt dann mit dem öffentlichen Schlüssel des Empfängers die Integritätsmeldung, worauf eine Entschlüsselung nur mit dem geheimen Schlüssel durch den Empfänger möglich ist. Die Rückmeldung wird von dem Empfänger der Nachricht mit dem öffentlich bekannten Schlüssel des Absenders verschlüsselt. Die erhaltene Rückmeldung kann der Absender mit seinem geheimen Schlüssel entschlüsseln.

Eine Weiterbildung des erfindungsgemäßen Verfahrens besteht darin, daß als Integritätsmeldung das Integritätsmerkmal und eine Transaktionsvariable verschlüsselt und übertragen werden. Die Transaktionsvariable kann dabei als Zufallszahl beim Absender erzeugt werden und dient im wesentlichen dazu, die empfangene Rückmeldung dem jeweiligen Absende-Vorgang zuzuordnen und einzelne Rückmeldungen von mehrmals versandten Nachrichten voneinander zu unterscheiden.

Eine andere Weiterbildung des erfindungsgemäßen Verfahrens besteht darin, daß absenderseitig ein Teil der Nachricht aus der Nachricht entfernt und innerhalb der Integritätsmeldung verschlüsselt und übertragen wird. Damit wird zusätzlich die Auswertung der empfangenen Nachricht erschwert, wenn die Integritätsmeldung nicht empfangen bzw. entschlüsselt werden kann. Das Erkennen der empfangenen Nachricht kann sogar ganz unmöglich gemacht werden, wenn gemäß einer vorteilhaften Ausführungsform des erfindungsgemäßen Verfahrens die Nachricht ebenfalls verschlüsselt und/oder signiert übertragen wird.

In manchen Fällen wird es genügen, die empfangene Rückmeldung mit der bis zum Empfang der Rückmeldung gespeicherten Integritätsmeldung zu vergleichen und damit den ordnungsgemäßen Empfang festzustellen. In der Regel ist jedoch auf Seiten des Absenders eine sichere Dokumentation erforderlich. Dazu kann bei dem erfindungsgemäßen Verfahren vorgesehen sein, daß die vom Absender empfangenen Rückmeldungen zusammen mit den absenderseitig abgeleiteten Integritätsmeldungen in einer Datenbank beim Absender gespeichert werden. Insbesondere eine Verfälschung der gespeicherten Daten, um möglicherweise den Empfang einer nicht abgesandten Nachricht nachträglich zu dokumentieren, kann bei dem erfindungsgemäßen Verfahren dadurch verhindert werden, daß die Rückmeldungen vom Empfänger signiert werden.

Eine Verbesserung bei der praktischen Durchführung des Verfahrens sowie eine bessere und sichere Dokumentation wird bei einer Weiterbildung des Verfahrens dadurch ermöglicht, daß mit der Integritätsmeldung und/oder der Rückmeldung weitere Informationen übertragen werden.

Häufig werden vertrauliche Nachrichten mit Hilfe von Personen ausgetauscht, die keine Berechtigung zur

Kenntnisnahme dieser Nachrichten haben. Bei dem postalischen Versand von derartigen Nachrichten werden dann mehrere Umschläge ineinander gesteckt. Bei dem erfindungsgemäßen Verfahren kann dieser Vorteil dadurch erzielt werden, daß die zu übertragenden Nachrichten — gegebenenfalls mehrfach — verschlüsselt werden. Hat beispielsweise eine Sekretärin die Berechtigung zum Entschlüsseln des Integritätsmerkmals und der damit empfangenen zusätzlichen Informationen, nicht jedoch die Berechtigung zur Kenntnisnahme des übertragenen Dokuments selbst, können beispielsweise in der weiteren Information Anweisungen zur weiteren Bearbeitung des verschlüsselten Dokuments enthalten sein — beispielsweise der Name desjenigen Empfängers, der zur Entschlüsselung berechtigt ist.

Ein Ausführungsbeispiel der Erfindung ist in der Zeichnung anhand mehrerer Figuren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 die absenderseitigen Verfahrensschritte in Form eines Ablaufdiagramms und

Fig. 2 die empfängerseitigen Verfahrensschritte ebenfalls als Ablaufdiagramm.

Nach einem Start bei **1** (**Fig. 1**) wird bei **2** das zu sendende Dokument ausgewählt. Es wird davon ausgegangen, daß dieses Dokument bereits in einem Speicher vorhanden ist. Danach erfolgt bei **3** eine Signatur SIGN des Dokuments, worauf das signierte Dokument DS bei **4** verschlüsselt wird. Nach der Verschlüsselung ENC wird bei **5** das Integritätsmerkmal VAR aus dem verschlüsselten Dokument DSC gebildet. Bei **6** wird ein Teil IK des Dokuments aus dem verschlüsselten Dokument DSC herausgetrennt.

Im Schritt **7** wird eine Transaktionsvariable TAV gebildet, worauf bei **8** zusätzliche Information ADINFO eingelesen wird. Diese zusätzliche Information enthält beispielsweise das Datum und die Uhrzeit oder wahlweise eingebbare Information.

Die bei **5** bis **8** gebildeten Daten werden im Schritt **9** zu einer Datei E zusammengefaßt, die im folgenden in Anlehnung an postalische Verfahren auch Umschlag (E = Envelope) genannt wird. Bei **10** erfolgt eine Signatur des Umschlags durch den Absender bzw. eine von ihm mit dem Absenden des Dokuments betraute Person. Danach wird bei **11** der signierte Umschlag ES verschlüsselt und als ESC bei **12** zusammen mit dem verschlüsselten Dokument abgesendet.

Bei **13** (**Fig. 2**) beginnt das Verfahren beim Empfänger, worauf bei **14** auf den Empfang eines Dokuments DSC mit einem Umschlag ESC gewartet wird. Das Eintreffen einer solchen Nachricht wird bei **15** auf einem Display angezeigt. Bei **16** erfolgt eine Entschlüsselung DEC des empfangenen Umschlags, wodurch die bei **17** durchgeführte Restaurierung des Dokuments möglich wird. Das restaurierte verschlüsselte Dokument DSC wird bei **18** decodiert und kann in geeigneter Form dem Empfänger zugänglich gemacht werden, beispielsweise am Bildschirm oder durch einen Ausdruck. Ferner kann die Signatur geprüft werden.

Im Schritt **19** wird aus dem empfangenen und bei **17** restaurierten Dokument DSC ein Integritätsmerkmal VAR nach dem gleichen Algorithmus wie im Schritt **5** beim Absender gebildet. Bei **20** werden VAR und VAR' miteinander verglichen. Sind beide Integritätsmerkmale verschieden, wird dieses bei **21** als Fehlermeldung ERROR angezeigt. Bei Gleichheit wird jedoch bei **22** zusätzliche Information ADINFO ausgegeben. Bei **23** wird eine Kurznachricht ADINFO für die Rückmeldung gebildet, die außer dem Empfangsdatum noch individuelle Nachrichten enthalten kann. Die Kurznachricht wird bei **24** mit VAR und der empfangenen Transaktionsvariablen TAV zu einer Rückmeldung zusammengesetzt.

Die Rückmeldung wird bei **25** signiert, bei **26** verschlüsselt und schließlich als RSC bei **27** zum Empfänger zurückgesendet. Die Rückmeldung wird beim Öffnen des empfangenen Umschlags immer automatisch erzeugt. Das Absenden der Rückmeldung geschieht beim dargestellten Ausführungsbeispiel nicht automatisch und zwangsläufig, sondern kann durch den Empfänger des Umschlags oder der Nachricht entweder durchgeführt oder unterlassen werden.

Die bei **28** (**Fig. 1**) empfangene, signierte und verschlüsselte Rückmeldung RSC wird bei **29** entschlüsselt und bei **30** mit den gespeicherten Daten VAR und TAV verglichen. Sind diese identisch, erfolgt eine entsprechende Anzeige bei **31**. Bei **32** wird der gesamte Vorgang in einem Speicher abgelegt. Sind die Daten jedoch nicht identisch, so erfolgt bei **33** eine Fehlermeldung.

Patentansprüche

1. Verfahren zur integren und authentischen Bestätigung des Empfangs einer von einem Absender an einen Empfänger übertragenen Nachricht, **dadurch gekennzeichnet,**
   - daß absenderseitig aus der Nachricht ein Integritätsmerkmal abgeleitet wird, das als Integritätsmeldung für den Empfänger entschlüsselbar verschlüsselt zum Empfänger übertragen wird,
   - daß empfängerseitig das verschlüsselte Integritätsmerkmal entschlüsselt wird,
   - daß aus der empfangenen Nachricht mit dem sendeseitig angewandten Algorithmus das Integritätsmerkmal abgeleitet wird,
   - daß das entschlüsselte und das empfängerseitig abgeleitete Integritätsmerkmal miteinander verglichen werden und
   - daß bei Übereinstimmung eine Rückmeldung an den Absender übertragen wird, die in für den Absender entschlüsselbarer verschlüsselter Form das Integritätsmerkmal enthält.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß als Integritätsmeldung das Integritätsmerkmal und eine Transaktionsvariable verschlüsselt und übertragen werden.

3. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß absenderseitig ein Teil der Nachricht aus der Nachricht entfernt und innerhalb der Integritätsmeldung verschlüsselt und übertragen wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Nachricht ebenfalls verschlüsselt und/oder signiert übertragen wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die vom Absender empfangenen Rückmeldungen zusammen mit den absenderseitig abgeleiteten Integritätsmeldungen in einer Datenbank beim Absender gespeichert werden.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß die Rückmeldungen vom Empfänger signiert werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß mit der Inte-

gritätsmeldung und/oder der Rückmeldung weitere Informationen übertragen werden.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 196 04 150 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 7. August 1997

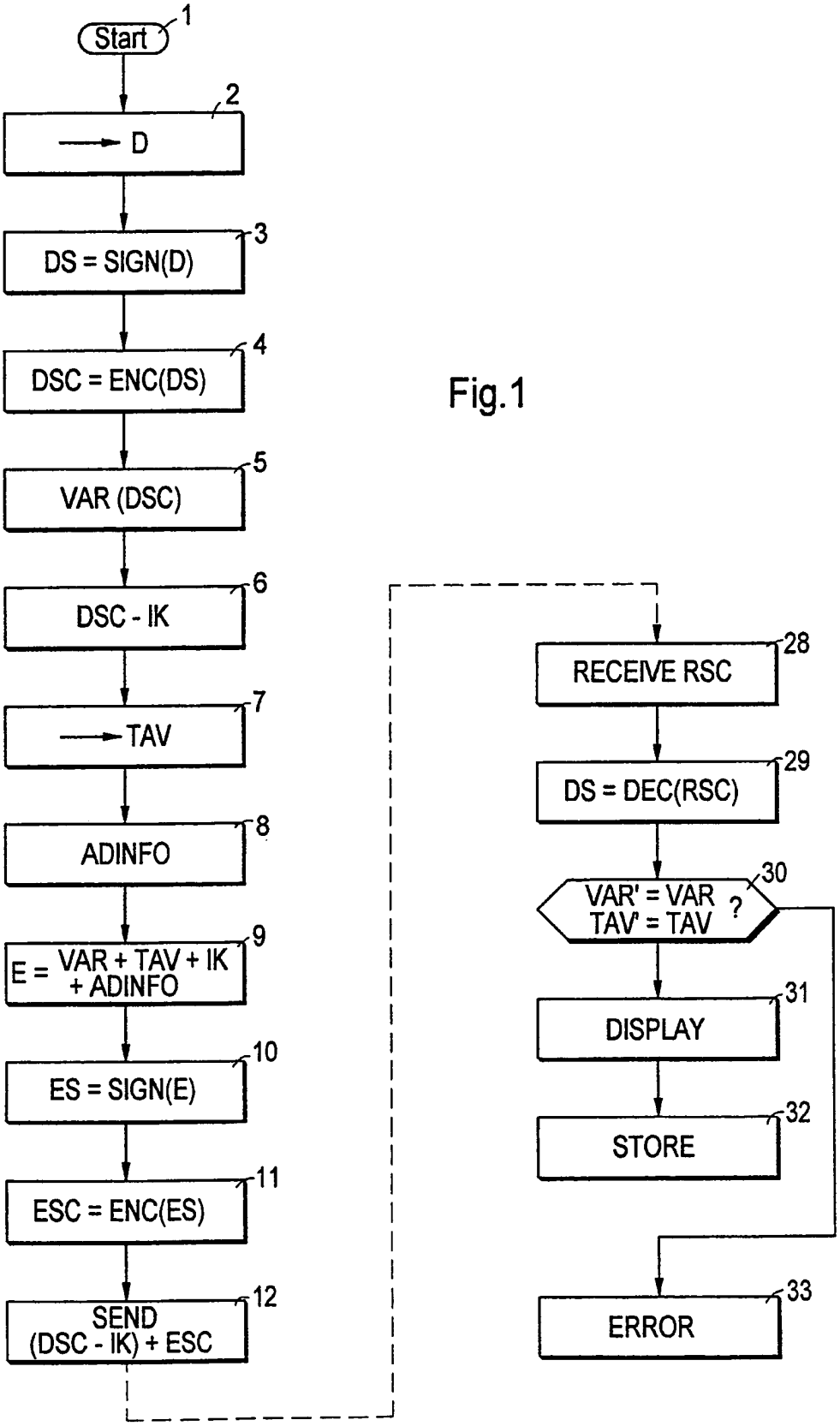


Fig.1

Nummer: DE 196 04 150 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 7. August 1997

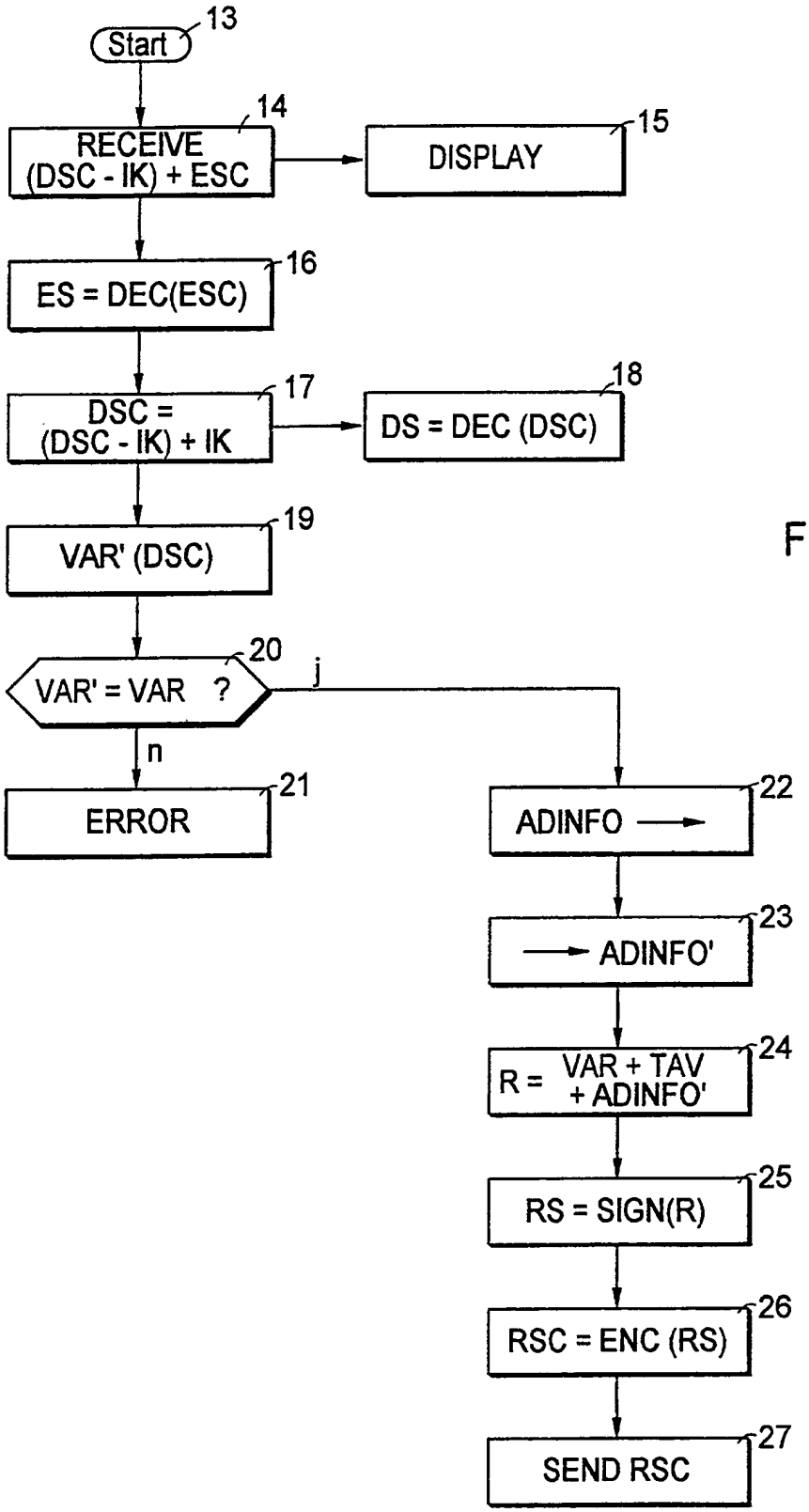


Fig.2